REMARKS

On page 2 of the Office Action, the Examiner rejected claims 15-20 as being directed to non-statutory subject matter. Applicants have amended claims 15-20 to recite an article of manufacture. Hence, claims 15-20 are directed to statutory subject matter.

On pages 2-5 of the Office Action, the Examiner rejected claims 15-20 under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 15, 16, 17, and 20 have been amended to overcome the rejection.

On pages 5-8 of the Office Action, the Examiner rejected claims 15-18, 20-26, and 28 under 35 U.S.C. §102(e) as being anticipated by Rothermel.

Rothermel describes a network security device management system 100 that includes a security policy manager device 110 able to communicate with a supervisor device 120. The supervisor device 120 is associated with a network security device (NSD) 130. The NSD 130 protects a trusted device 220 from an external device.

The NSD 130 stores information about the supervisor device 120 (e.g., the device's network address) with specific security policy information 133. The NSD 130 also stores any required access information (such as a unique password which the supervisor device

120 must provide in order to gain access to the NSD 130) along with device access information 134. The NSD 130 implements a security policy by executing software 132 and using the stored specific security policy information. An example of a security policy is the following: outgoing FTP connections are allowed only from certain information services associated with IP addresses 220.15.23.52, 220.15.23.53, and 220.15.23.97.

Figures 5A-5D provide an example of a GUI displaying a hierarchical view of a supervisor device, a NSD, and corresponding configuration and network information. As shown in Figure 5A, various information about the supervisor device and the NSD can be displayed textually (e.g., the IP address, connection status, and phone number). Figure 5B provides a graphical view of real-time connections, Figure 5C indicates various users associated with specific IP addresses, and Figure 5D includes information about IP addresses and ports which are currently blocked.

As shown in Figure 6, the NSD software components include a packet filter engine 615 and authentication software 640. The packet filter engine 615 implements the security policy for the NSD. A network security information logging component 660

provides network security information to the supervisor device.

Figure 7 is a flow diagram of a routine 700 executed by the NSD. The routine 700 implements a specific security policy for the NSD by monitoring network information passing between devices of interest (e.g., between an external device and a trusted device), by applying security policy filter rules, and by generating network security information about events of interest.

At 705, the NSD loads its software. At 710, the NSD loads NSD-specific network packet filter rules that will be used to implement the specific security policy. At 715, the NSD monitors any passing network information. At 720, when network information packets of interest are detected, the NSD filters the network information packets. At 725, the NSD generates network security information about any events of interest. At 730, the NSD responds to management messages from the supervisor device. At 790, the NSD determines whether to continue monitoring network information packets.

Figure 8 shows the network packet filtering at 720. The NSD determines whether network information packets match one or more security policy filter rules,

applies filter rules to determine what actions to take for the packets, and takes the action. At 805, the NSD receives information about the network information packets of interest. At 810, the NSD determines whether the packets match a filter rule. If so, the NSD at 815 applies the filter rule to determine an action to be taken for the packets. If the NSD determines at 810 that no filter rule applies, the NSD at 820 determines a default action to be taken for the packets. Default actions include denying passage of all packets that are not explicitly approved, blocking spoofing attacks, blocking port space probes, and blocking address space probes. At 825, the NSD takes the determined action on the packets.

Independent claim 15 - As can be seen, Rothermel fails to disclose identifying ID information from the packets in order to identify a user, acquiring attribute data corresponding to the ID information, and determining whether the packets are valid based on determination rules that correspond to the attribute data.

The Examiner asserts that the acquiring of attribute data corresponding to a user ID is disclosed in

Rothermel at column 7, lines 50-53, and at column 2, lines 15-23, at column 4, lines 49-56, and in Figure 5c.

However, column 7, lines 50-53 merely state that the NSD implements a security policy by executing software and by using stored policy information. There is no disclosure in Rothermel that either the software or the stored policy information associates user attributes with user identities. Indeed, the policy information shown in Rothermel (i.e., 316 of Figure 3B) identifies IP addresses and a rule but not with users or user attributes. Again, there is no disclosure here of associating user attributes with user identities and using the user attributes with the stored rules to make data validity determinations.

Column 2, lines 15-23 state that the decision to take different actions can also be based on additional factors such as the direction of information flow, or on the basis of the sender or the intended recipient of the information. Again, there is no disclosure here of associating user attributes with user identities and using the user attributes with the stored rules to make data validity determinations.

Column 4, lines 49-56 state that security policy templates are defined by a user of the manager

device (i.e., the system administrator) and are used to implement consistent network security policies across multiple NSDs while reducing the risk of configuration error. Each template defines default network information filtering rules for various common services and protocols, and further defines aliases for representing various specific devices of interest to the NSD. Yet again, there is no disclosure here of associating user attributes with user identities and using the user attributes with the stored rules to make data validity determinations.

Finally, Figure 5C shows various users associated with specific IP addresses. That sentence is all Rothermel has to say about any connection between users and IP addresses. Thus, Rothermel does not disclose that the user's ID is used to acquire an IP address from the table of Figure 5C and that acquired IP address is used with a corresponding rule to determine if a packet is valid.

Moreover, while the Examiner may argue that an IP address is an attribute of a network device, an IP address is not an attribute of the user.

Furthermore, even if column 2, lines 15-23 are read in conjunction with Figure 5C, one of ordinary skill

in the art would only conclude that the sender or recipient of column 2, lines 15-23 is merely a network device because the policies described in Rothermel merely associate rules with IP addresses and because an IP address is an attribute of the network device rather than a user. Indeed, Rothermel defines a sender or recipient at column 2, lines 15-23 and elsewhere as a network device.

Accordingly, for all of the above reasons, independent claim 15 is not anticipated by and is patentable over Rothermel.

Because independent claim 15 is not anticipated by and is patentable over Rothermel, dependent claims 16-18 are not anticipated by and are patentable over Rothermel.

For similar reasons, independent claims 20-23 and 28 are not anticipated by and are patentable over Rothermel.

Because independent claim 23 is not anticipated by and is patentable over Rothermel, dependent claims 24-26 are not anticipated by and are patentable over Rothermel.

On page 9 of the Office Action, the Examiner rejected claims 19 and 27 under 35 U.S.C. §103(a) as being unpatentable over Rothermel.

However, since independent claims 15 and 23 are patentable over Rothermel, dependent claims 19 and 27 are likewise patentable over Rothermel.

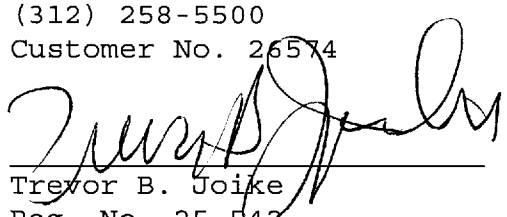
CONCLUSION

In view of the above, the claims of the present application patentably distinguish over the art applied by the Examiner. Accordingly, allowance of these claims and issuance of the present application are respectfully requested.

The Commissioner is hereby authorized to charge any additional fees that may be required, or to credit any overpayment, to deposit account No. 501519.

Respectfully submitted,

Schiff Hardin LLP
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
(312) 258-5500
Customer No. 26574

By: 
Trevor B. Joike
Reg. No: 25,542

December 22, 2008